REMARKS/ARGUMENTS

Status of application

The pending claims have been examined in stand rejected in view of prior art. The pending claims are amended to further clarify the claimed subject matter. This Amendment is filed in conjunction with a Request for Continued Examination (RCE). Accordingly, reexamination and reconsideration are respectfully requested.

Section 102 rejection

Claims 1, 2, 4-12, 18, 19, 21-29, 37, 38, and 41-48 are rejected under 35 U.S.C. § 102(a) as allegedly being anticipated by Jones et al. WIPO Pub. WO 03/030483 (hereinafter "Jones"). This rejection is respectfully traversed.

While the Office may apply to Applicants' claims the broadest reasonable meaning of the words in their ordinary meaning as they would be understood by one of ordinary skill in the art, any meaning must consider any definitions or other information in the written description of Applicants' specification. *See In re Morris*, 127 F.3d 1048, 1064 (Fed. Cir. 1997). As discussed below, Jones fails to anticipate or render obvious Applicants' claims.

CLAIM 1

Applicants independent Claim 1 now recites:

> A computer-implemented method for improving service accounting in a network, the method comprising the steps of:
> in response to a first Authentication, Authorization, and Accounting (AAA) server receiving a request to authorize a client to access a network resource,
> said first AAA server obtaining an accounting record for the client from an external resource communicatively coupled to the AAA server,
> said first AAA server authorizing said client to access the network resource based on said accounting record, and
> said first server sending a Remote Authentication Dial In User Service (RADIUS) protocol access accept message that includes the accounting record within the access accept message;
> causing the accounting record to be logged;
> a second AAA server receiving a RADIUS start session message that includes the accounting record within the start session message.

Applicants' Claim 1 has been amended to further clarify the claimed subject matter of Claim 1. In particular, in response to receiving a request to authorize a client **to access a network resource**, the AAA server obtains an accounting record for the client **from an external resource communicatively coupled to the AAA server**. For example, in one embodiment of

Claim 1, the external resource is a Lightweight Directory Access Protocol (LDAP) server coupled to the AAA server. *Applicant's specification*, paragraph [0035]. In Claim 1, the accounting record obtained from the external resource is used by the AAA server to authorize the client to access the network resource. The AAA server than sends a Remote Authentication Dial In User Service (RADIUS) access accept message that includes the accounting record used to authorize the client. The accounting record is subsequently received in a RADIUS start session message.

Often, an accounting record obtained from an external resource that is used by an AAA server to authorize a client to access a network resource contains information that is useful to include in logs maintained by various network devices participating in an AAA session. For example, the accounting record may include identity information associated with the authorized client. *Id.*, paragraph [0008-0012]. Logging information from such accounting records is useful for a number of reasons including aiding system debugging and identifying fraudulent users, analysis, audit, and reporting. *Id.*, paragraph [0006].

However, it is inefficient to obtain the accounting record from the external resource each and every time a network device wishes to add information from the accounting record to a log. *Id.*, paragraph [0014]. The various network devices might cache the accounting record after obtaining the accounting record from the external resource. *Id.*, paragraph [0013]. However, caching requires extra computing resources of the network devices. Further, caching is sub-optimal in load balanced environments. *Id.*, paragraph [0013].

Applicants' solution of Claim 1 allows an accounting record obtained from an external resource to be logged by various network devices throughout the network during an AAA session **without having to re-obtain the accounting record from the external resource and without having to cache the accounting record**. This is accomplished in part by the AAA server sending a RADIUS access accept message that includes the accounting record used by the AAA server to authorize the client in the access accept message thereby causing the accounting record to be logged. Jones, on the other hand, does not describe "said first server sending a Remote Authentication Dial In User Service (RADIUS) protocol access accept message that includes the accounting record within the access accept message", as claimed or "causing the accounting record to be logged", as claimed.

Jones describes session management for wireless networks which are administered by an Authentication, Authorization, and Accounting (AAA) server. *Jones*, col. 5, lines 10-15. When the AAA server of Jones receives a request to authorize a data session for a mobile node the

AAA server performs "some manner of lookup" or the "usual authentication and authorization process" to determine whether the data session for the mobile node should be allowed. *Jones*, col. 10, lines 24-25; col. 11, line 27; fig. 5 steps 84 and 98. If the AAA server determines that the data session should be allowed, then:

- the AAA server checks for the existence of a pre-existing data session for the mobile node; and
- if there is a pre-existing data session for the mobile node, the AAA server sends a RADIUS access accept message that includes a data session identifier for the data session.

(*Jones*, col. 11, line 25 – col 12, line 11; fig. 5 steps 98, 100, 102, and 104).

The data session identifier sent in the access accept message in Jones is used by wireless device service providers to manage data sessions of mobile devices as they roam from network to network. The identifier allows an AAA server to detect and terminate stale data sessions even if the mobile device is dormant when it moves from one network to another network. *Jones*, col. 7, lines 10-20.

It is the data session identifier that Jones includes in an access accept message that the Office Action equates with Applicant's "accounting record". However, unlike Applicants' "accounting record", Jones' data session identifier is not used to "authorize" a client to access a network resource, as claimed. This is clear from the description in Jones. Specifically, Jones states at col. 11, lines 22-33:

> The mobile node 54'contacts the PDSN B 82 and the PDSN B 82 sends a RADIUS access request message to the stateful RADIUS server 62 at, step 98, requesting authorization to setup the data session for the mobile node 54' (note that a variety of techniques are known in the art for locating the home AAA server for a given mobile node). **On receipt of the access request message, the stateful RADIUS server 62 performs the usual authentication and authorization process, then checks for the existence of a pre-existing data session from the same mobile node 54', at step 100.** In the context of this example the stateful RADIUS server 62 locates the data session on PDSN A 58 in its cache and constructs a Class attribute containing the IP address of PDSN A 58 and the Acct-Session-Id of the data session on PDSN A 58. This Class attribute is appended to the access accept message returned to PDSN B 82 at step 102.

The above-cited portion of Jones makes clear that Jones checks for the existence of a pre-existing data session for a mobile node only **after** the AAA server has determined that the requesting entity is authorized to setup a data session for the mobile node. Thus, any information the AAA server in Jones obtains from a pre-existing data session is always obtained **after** authorization. Indeed, the AAA server in Jones will not send an access accept message and will

not check for the existence of a pre-existing data session if the mobile node is not **first** authorized by the AAA server. *Jones*, col. 10, lines 27-27. Thus, none of the information the AAA server in *Jones* obtains from a pre-existing data session is used for authorizing the mobile node.

The Office Action uses an unreasonably broad interpretation of "authorizing" to bring Jones' check for a pre-existing data session description within the meaning of "said first AAA server authorizing said client to access the network resource based on said accounting record", as claimed. As featured in Applicants' Claim 1 and as one skilled in the art would understand in light of Applicant's disclosure, "authorizing" in Claim 1 involves the AAA server determining whether the client should or should not be granted access to a particular network resource such as, for example, an application server. *See, e.g., Applicant's specification*, paragraphs [0003], [0037]. In particular, Claim 1 recites "said first AAA server **authorizing said client to access the network resource** based on said accounting record". *Emphasis added.* Thus, "authorizing" as featured in Applicant's Claim 1 does not refer to activity performed by the AAA server **after** the AAA server has already determined whether the client should or should not be granted access to a network resource. Further, activity performed by an AAA server that does not include determining whether a client should be granted access to a network resource is not "authorizing" as claimed.

In Jones, the AAA server has already determined whether the mobile node should be granted access to a network resource **before** the AAA server checks for the existence of a pre-existing data session. *Jones*, col. 11, lines 26-29. Thus, this post-authorization activity in Jones is not "authorizing" as claimed

Furthermore, in Jones, the existence or non-existence of a pre-existing data session has absolutely no effect whatsoever on whether the mobile node is or is not granted access to a network resource. Specifically, if, after the mobile has been authorized by the AAA server in Jones, a pre-existing data session for the mobile node is not identified, "then a regular response message would be returned". *Jones*, col. 6, line 17. In the context of RADIUS, the "regular response message" referred to at *Jones*, col. 6, line 17 is a RADIUS access accept message. *Jones*, col. 10, lines 25-30. If, on other hand, after the mobile node has been authorized, a pre-existing data session for the mobile node is identified, then a RADIUS access accept message is also returned. *Jones*, col. 11, lines 20-33. In other words, the existence or non-existence of a pre-existing data session has no impact on the prior authorization performed by the AAA server. Thus, it is unreasonable to characterize the check for a pre-existing data session in Jones that is

only performed **after** the mobile node has been authorized as "authorizing" as claimed.

Because Jones' check for a pre-existing data session occurs only after the mobile node has been authorized and because Jones' check for a pre-existing data session is not in any way used to authorize the mobile node to access a network resource, the information from the pre-existing data session that Jones sends in an access accept message is not an "accounting record" as claimed. Thus, because Jones does not send an "accounting record" in an access accept message, Jones does not describe "said first server sending a Remote Authentication Dial In User Service (RADIUS) protocol access accept message that includes the accounting record within the access accept message", as claimed.

Further, Jones has no mention of a "log" or "logging" that could be relevant to the feature of Applicants' Claim 1 reciting "causing the accounting record to be logged". This is unsurprising because Jones is not directed to techniques for logging within a network.

With respect to the Claim 1 feature "causing the accounting record to be logged", the Office Action cites to Jones at col. 10, lines 23-35. The cited portion of Jones states, in its entirety:

> First, at step 84, the PDSN A 58 transmits an access request message to the stateful RADIUS server 62. The stateful RADIUS server 62 then performs some manner of lookup at step 85 to establish whether the communication should be allowed. If it is determined that communication should proceed, then an access accept message returned to PDSN A 58 at step 86. Following successful initialization of the data service PDSN A will send an Accounting Start message to the RADIUS server at step 87. This message contains an Acct-Session-Id attribute which in conjunction with the IP address of PDSN A 58 serves to uniquely identify the data session network-wide. On receipt of the accounting start message, the stateful RADIUS server 62 creates a new session record in its cache to track the data session on PDSN A (step 88). A session key is formed from the Acct-Session- Id attribute and the IP address of PDSN A. The session key and mobile node identifier are stored in the new session record. Communication would then proceed,

As explained above, Jones' session record is not an "accounting record" as claimed. Thus, to the extent that Jones describes "logging" the session record, any such description does not describe "causing the **accounting record** to be logged" (emphasis added) as claimed.

Claim 1 represents a patentable advance over the prior art. For example, by performing the method of Claim 1, an AAA server can keep a more detailed log of the data obtained from an external resource used to authorize a client to access a network resource without needing to cache the data at the AAA server and without having the AAA server perform multiple reads from the external resource. More generally, the method of Claim 1 provides sufficient accounting information for creating useful log records while at the same time allowing AAA

servers to be stateless, load balanced, and less burdened. Such advantages are not possible with the mobile node session tracking approach of Jones which does not perform "said first server sending a Remote Authentication Dial In User Service (RADIUS) protocol access accept message that includes the accounting record within the access accept message" as claimed or perform "causing the accounting record to be logged" as claimed.

Based on the foregoing, Applicant respectfully submits that Claim 1 is allowable over Jones.

CLAIM 18

Applicants' independent Claim 18 contains recitations similar to those of independent Claim 1 discussed above. Accordingly, Claim 18 is allowable for at least the same reasons that Claim 1 is allowable.

The preamble of claim 1 eliminates material the Applicants have found unnecessary. Certain claims recite features for purposes of expressing context and the capabilities of certain steps, but infringers are not required to provide all such features. For example, infringing embodiments should have the capability to interact with a network resource, external resource, client, logging device, and network device, in the manner claimed, but an infringer is not required to make, use, sell or import those features; they could be provided by third parties.

Section 103 rejection

Claims 3 and 20 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Jones in view of U.S. Patent Pub. No. 2003/0035409 (hereinafter "Wang"). This rejection is respectfully traversed.

Here, the Office Action repeats the rejection under Jones, but adds Wang for the prospect of teaching additional accounting record limitations such as those raised in the Claim 3 limitation of "obtaining the accounting record for the client from a Lightweight Directory Access Protocol directory."

Applicants' independent claims 1 and 18 are allowable for at least the reasons stated above pertaining to the rejection based on Jones. Applicants' invention of claims 1 and 18 is directed to a solution that provides sufficient accounting information for creating useful log records while at the same time allowing AAA servers to be stateless, load balanced, and less burdened. The combination of Jones and Wang proposed in the Office Action at best is merely duplicative of what Applicants have already disclosed in the Background of their specification

(See Applicants' specification, paragraph [0008] describing how AAA servers may need to access an external identity repository such as an LDAP server). Nothing in Wang cures the deficiencies of Jones disclosed above with respect to the features of independent Claims 1 and 18 discussed above with respect to the Section 102 rejection. Accordingly, it is respectfully submitted that the pending claims are patentable under Section 103.

Conclusion

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a check for the petition for extension of time fee and other applicable fees is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: March 1, 2010

/AdamCStone#60531/

Adam C. Stone
Reg. No. 60,531

2055 Gateway Place Suite 550
San Jose, California 95110-1093
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076